Beim Bearbeiten des Arbeitsblattes „Asymmetrische Kryptographie“ hatten wir zuletzt gesehen, dass sich Public-Key-Verfahren wie RSA nicht zur Verschlüsslung von großen Datenmengen eignen.

In der Praxis kommen daher für einen einzigen Datentransfer sowohl symmetrische als auch asymmetrische Verfahren zum Einsatz. Dabei wird wie folgt vorgegangen:

1. Unter Verwendung von Public-Key-Verfahren (z.B. RSA) wird zunächst ein symmetrischer Schlüssel ausgetauscht.
2. Die Nutzdaten werden anschließend mit dem symmetrischen Schlüssel verschlüsselt und übertragen.

Aufgabe 1

Nutzen Sie Ihre „Public-Key-Infrastruktur“ aus dem Aufgabenblatt „Asymmetrische Kryptographie“ und durchlaufen Sie das folgende hybride Protokoll.

1. Erzeugen Sie zunächst einen „zufälligen“ symmetrischen Schlüssel mit dem Befehl:

   ```
   openssl rand -base64 32 > key.bin
   ```

2. Verschlüsseln Sie anschließend diesen symmetrischen Schlüssel mittels RSA, nutzen Sie dabei den öffentlichen Schlüssel desjenigen, mit dem Sie kommunizieren möchten.

   ```
   openssl rsautl -encrypt -inkey FritzMuellerPublic.pem -pubin -in key.bin -out key.bin.enc
   ```

3. Verschlüsseln Sie die “Nutzdaten” mittels des symmetrischen Schlüssels

   ```
   openssl enc -aes-256-cbc -salt -in einFilm.avi -out einFilm.avi.enc -pass file:key.bin
   ```

4. „Senden“ Sie die Dateien `key.bin.enc` und `einFilm.avi.enc` über das Tauschlaufwerk an den Empfänger (indem Sie ein passendes Unterverzeichnis anlegen z.B. „`anFritzMueller`“).

5. Die Aufgabe gilt als absolviert, sobald der Empfänger Ihre Nutzdaten mit den folgenden Befehlen erfolgreich dechiffrieren kann:

   ```
   openssl rsautl -decrypt -inkey private.pem -in key.bin.enc -out key.bin

   openssl enc -d -aes-256-cbc -in einFilm.avi.enc -out einFilm.avi -pass file:key.bin
   ```

Aufgabe 2

Überlegen Sie sich wie ein „Hacker“ das folgende Protokoll (aus dem Übungsblatt „Asymetrische Kryptographie“) erfolgreich angreifen könnte.

1. Alice macht Bob Ihren öffentlichen Schlüssel bekannt
2. Bob benutzt diesen Schlüssel (also den öffentlichen Schlüssel von Alice) um seine Nachricht an Alice zu verschlüsseln
3. Alice benutzt Ihren geheimen Schlüssel um die Nachricht, die Bob zuvor mit Ihrem öffentlichen Schlüssel verschlüsselt hat zu entschlüsseln. Da nur Sie Ihren privaten Schlüssel kennt, und nur dieser Schlüssel dazu geeignet ist die Nachrichten von Bob zu entschlüsseln, kann nur Alice die Nachricht dechiffrieren.

Sollten Sie nicht selbst auf die Lösung kommen, so grämen Sie sich nicht zu sehr. In der „Community“ der Kryptographen hat es immerhin 17 Jahre gedauert bis der Angriff publik wurde.

Recherchieren Sie stattdessen im Internet nach „man in the middle“.